Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Consumers from SIM Swap and Port-Out Fraud	)	WC Docket No. 21-341
	)	

VERIZON COMMENTS

The Commission's rules and policies surrounding the transfer of services and devices have long recognized the importance of both customer choice and security.[1] A seamless process benefits competition and customer choice by enabling consumers to efficiently switch providers and take advantage of new devices and service plans. Yet it may create opportunities for bad actors to engage in fraudulent activities that compromise consumers' privacy, account security, and financial interests.

Policymakers are rightfully concerned about the types of fraud described in the *NPRM*.[2] Verizon works aggressively to protect its consumer and business customers from bad actors who attempt to exploit the processes of transferring service between SIMs ("SIM changes") and porting telephone numbers. Several *NPRM* proposals would ratify many of the measures Verizon and others have taken to protect consumers. But fraudsters are sophisticated and constantly look to circumvent any protections, no matter how robust. Any new rules should thus afford providers with the flexibility to nimbly prevent, detect, and respond to fraudulent activities, while not

---

1 *See Telephone Number Portability*, 18 FCC Rcd 20971, ¶ 18 (2003); *Local Number Portability Porting Interval and Validation Requirements*, 25 FCC Rcd 6953, ¶¶ 16, 21 (2010); *Service Rules for the 698-746, 747-762 and 777- 792 MHz Bands*, 34 FCC Rcd 5134, ¶ 10 (2019) ("strict compliance with" device unlocking rule "facilitates and may even encourage fraud"); *see also* Report and Order, 14 FCC Rcd 1508, ¶ 16 (1998) (rules prohibiting slamming "may also make it more difficult for carriers to gain new subscribers in a legitimate manner").

2 *Protecting Consumers from SIM Swap and Port-Out Fraud, Notice of Proposed Rulemaking*, WC Docket No. 21-341, FCC 21-02 (Sept. 30, 2021) ("*NPRM*").

unnecessarily burdening customers during the overwhelming majority of legitimate SIM change and porting transactions.

I. ANY NEW RULES ON SIM CHANGES SHOULD PRESERVE PROVIDERS' FLEXIBILITY AND ABILITY TO STAY AHEAD OF BAD ACTORS.

SIM changes help customers by enabling them to easily move a mobile phone number to a new SIM card, for example when they need to use a new device, and facilitate competition among service providers and device manufacturers. Verizon guides customers through the process easily and securely.[3] The overwhelming number of SIM changes Verizon processes are legitimate and, for the relatively few that are not, Verizon's security methods reflect "reasonable measures" to address unauthorized SIM changes. Through these measures Verizon efficiently and effectively monitors, detects, and can respond to a constantly changing field of fraudulent activities, ensuring not only the protection of CPNI, but customers' other privacy and security interests as well.

A. Strong Customer Care and Employee Training Programs Are Critical.

Verizon diligently addresses fraudulent SIM changes through methods that account for the differences between postpaid and prepaid customers, between individual consumer and enterprise customers, and the risks associated with each. Customer care and employee training programs are critical for preventing and identifying unauthorized and high-risk SIM changes for postpaid customers.[4] Verizon's general customer care efforts include procedures like encouraging consumers to download and set up the MyVerizon app to enable important protection features and push notification-based authentication. Using the app, customers may easily establish two-factor authentication for online account and customer care access while also

---

3 *See* https://www.verizon.com/support/4g-sim-card-faqs/.

4 *See NPRM* ¶¶ 38-39.

using locally-stored biometric information (e.g., device-native fingerprint or faceprintID) to securely log into the app. Verizon customer care representatives also encourage customers to verify the email address associated with their accounts to confirm its accuracy and help secure the customer's account privacy. And account owners are encouraged to assign roles and privileges to mobile lines on their account and to restrict the most significant account management tasks to designated account managers (rather than all account members).[5]

Verizon also trains all customer care employees to identify and prevent unauthorized SIM change attempts through the use of multiple authentication protocols. Verizon makes all efforts to properly authenticate customers and minimizes the number of employees who have a legitimate business need to access accounts without customer authentication.[6] Two-employee sign-off can be appropriate in circumstances when other authentication methods are unavailable, and Verizon trains select employees to assist customers this way. Customer care employees identifying potentially fraudulent SIM changes refer those reports to dedicated investigative teams. And there is a toll-free number for customers to contact or obtain assistance from Verizon in the event of an unauthorized SIM change.

B. Verizon's Methods of Preventing Fraudulent SIM Changes Have Evolved and Improved to Better Protect Customers.

Verizon already employs (or is on track to employ) many of the methods identified in the *NPRM*, such as notifying customers of high-risk SIM change authentication attempts, failed or otherwise, and of other account changes.[7] Verizon already restricts use of call detail for customer

---

[5] Many of Verizon's security-related efforts for both SIM changes and port-out fraud are described on its website, see www.verizon.com/support/keeping-your-account-safe-faqs/ and www.verizon.com/about/account-security/account-take-over/.

[6] *See NPRM* ¶¶ 22, 38.

[7] *See id.* ¶ 22.

authentication (including for prepaid).[8] While SIM change fraud has historically targeted postpaid service, safeguards also are in place for prepaid customers.[9] A service provider will have limited information about the prepaid customer and, in many cases, about the customer's device. Even so, Verizon only allows authentication using reliable, available methods, and has begun integrating its prepaid offerings (including the Visible brand) more closely into the authentication security systems used for postpaid customers to further align and improve our methods to prevent to fraudulent activity.

With regard to transparency, as noted earlier Verizon provides information for customers on its websites about the risk of SIM change fraud and the steps customers can take to protect themselves. In practice, all SIM change attempts are monitored, and unauthorized changes are reported to the FCC/FBI/USSS portal (insofar as CPNI might have been affected). And when Verizon becomes aware of fraud, we notify customers as appropriate and can provide them and law enforcement with sufficient information to mitigate the impact. These customer notifications have not raised law enforcement concerns and the Commission should revisit its seven-day notification delay rule so providers may quickly notify customers of a confirmed CPNI breach so they can take immediate steps to protect other accounts.[10]

C. Any New Rules Should Give Wireless Providers Flexibility to Keep Ahead of Bad Actors.

The *NPRM* implies a tension between regulatory certainty and the risk of giving bad actors a "roadmap" for future actions. It would create a new duty to use "a secure method of authenticating its customer" before "effectuating a SIM change" and deem any one of four

---

8 *See id.* ¶ 30.

9 *See id.* ¶ 45.

10 *See id.* ¶ 68; 47 C.F.R. § 64.2011(b).

separate methods as compliant—essentially a safe harbor approach. Yet it also states "that carriers have statutory duties to protect the confidentiality of their customers' private information and to maintain just and reasonable practices and that these statutory duties are not necessarily coterminous with our rules"—suggesting that additional measures may be needed.[11]

In fact, providers must have flexibility both to develop and implement new methods beyond those enumerated in the draft rule to keep ahead of bad actors and to abandon measures that no longer work. An overarching duty to use a secure method (or combination of methods) to prevent unauthorized SIM changes would best achieve this goal, without the need to enumerate particular methods that will give bad actors a roadmap and that may prove less effective over time. While the proposed rules would not restrict service providers from using other secure authentication methods, the Commission should not presume or signal that alternative methods are necessarily less secure.

For example, while the *NPRM* questions the use of SMS, it can be an effective authenticator (including for port-outs).[12] In many cases email is also an effective and necessary method of authentication. And while recent payment information, standing alone, could be considered an insufficient authentication tool, if it corroborates other strong indicators it could still be useful.[13] Likewise, an account freeze or lock may be superfluous or of limited interest to consumers given the corresponding need for rigorous authentication to remove the freeze or lock.[14] And requiring each line on a family or multi-line business account to have its own

---

11 *See NPRM* ¶ 22 n.66.

12 As the Federal Trade Commission has found, in some cases "use of SMS text messages as a factor may be the best solution because of its low cost and easy use …." www.ftc.gov/system/files/documents/federal_register_notices/2021/10/safeguards_rule_final.pdf

13 *NPRM* ¶¶ 30, 33.

14 *See id.* ¶ 39.

passcode could unnecessarily burden customers by preventing a customer from using a spouse's device to complete a SIM change for a lost device, or unnecessarily complicating a business administrator's ability to manage the account.[15]

Delaying SIM changes after multiple failed authentication attempts, as well as notifying the customer of attempted and/or executed SIM changes, can be useful tools in some cases, particularly where analytics identify high risk transactions that may warrant further measures like these. But again, the vast majority of transactions are legitimate and the potential adverse impact on those SIM changes—often needed for a lost or stolen phone—will weigh against a delay in many cases.[16]

Flexibility is also warranted for other customer notification issues raised in the *NPRM*. Prescriptive rules for the content and delivery method of the notification are unnecessary. Providers also should have discretion to use a push notification together with supplemental verification methods to stop a high risk transaction. And regular mail can be problematic, as it could cause confusion when delayed or if it arrives after an electronic notification.[17]

Importantly, the Commission should clarify the scope of transactions covered by any new rules. The *NPRM* focuses on higher-risk SIM changes, but a "SIM change" occurs whenever a mobile number is reattributed to a new SIM for a simple device upgrade. The vast majority of SIM changes do not raise security concerns. As the *NPRM* notes, in-store customers in need of a SIM change may not be tech savvy, so flexibility to allow some form of physical documentation will be needed.[18] In addition, any rules should be competitively neutral, including for MVNOs,

---

15 *See id.* ¶ 40.

16 *See id.* ¶¶ 33-35, 37.

17 *See id.* ¶ 36.

18 *See id.* ¶ 31.

which control their own mobile device sales and customer terms of service. And rules may be appropriate for mobile or nomadic VoIP providers offering products that rely on SIM cards.[19]

In assessing the reasonableness of a service provider's authentication method(s) in a given SIM change scenario, the safeguards of third party institutions with whom the customer does business also are relevant. While a wireless provider's practices could prove to be reasonable, effective and thorough, the fraud prevention practices of the customer's financial institution, or the customer's email provider, may not. Wireless customers can take advantage of service provider's more robust authentication protections, with engagement of third parties that will similarly protect their identity and other personal information. Financial and other institutions should employ better solutions like ZenKey and other service provider-supported verification tools, requiring the utilization of device enabled two-factor authentication for a secured process which requires an owner-possessed mobile device to complete verification.

Finally, the industry's experience with SIM changes and porting fraud warrants a fresh look at the current CPNI rules for customer authentication—which are almost fifteen years old. Many customer authentication and security tools have surpassed the effectiveness of those rules, some of which add significant burden to providers and customers with little if any corresponding benefit. To keep ahead of bad actors, providers need flexibility to employ other more secure alternatives to passwords and government-issued IDs.[20] The current rules require not only authentication, but authentication in a particular way. For example, requiring a password for a customer's online access to CPNI may have been state-of-the-art at one time, but security methods have evolved since then and will continue to do so. The Commission should thus align

---

19 *See id.* ¶ 44.

20 An ID also may not be relevant for business customers whose personal contact detail will not match their business contact detail.

the existing authentication rules to the *NPRM*'s flexible, non-prescriptive approach by requiring providers to use security authentication methods for CPNI access without dictating the provider's method. The rules could continue to list authentication through a photo ID and/or a password as a possible means of authentication but the Commission should make clear that alternative authentication techniques may be acceptable as well.

II. ANY RULES SHOULD PRESERVE SERVICE PROVIDERS' AUTHORITY TO USE TARGETED MEASURES THAT DO NOT HINDER LEGITIMATE PORTS.

Verizon aggressively monitors port-out fraud and uses well-established and innovative methods to combat it. Today's regulatory framework gives Verizon the flexibility to pursue these actions. Codifying aspects of the wireless industry's port authentication practices could provide a degree of regulatory certainty but, as with SIM changes, wireless providers should remain free to pursue more robust authentication measures as bad actors' practices mutate over time.

A. Verizon Has Substantially Reduced Incidents of Porting Fraud Under the Existing Local Number Portability Rules.

As with SIM changes, Verizon already uses many of the authentication safeguards for number porting transactions described in the *NPRM*, and generally supports two-factor authentication. ZenKey is one of many available tools to enhance security and modules of that application are incorporated into the MyVerizon app for consumers.[21] Verizon's number porting group diligently pursues reports of unauthorized ports and works with other providers to retrieve numbers and correct the affected account, and Verizon's security organization analyzes these incidents to determine whether additional safeguards are warranted.

Last year, Verizon initiated the use of a transaction-specific "Number Transfer PIN" (NTP) for postpaid consumers to provide to their new provider to initiate the porting process.

---

21 *NPRM* ¶ 54.

This helped substantially reduce incidents of port-out fraud. We socialized the NTP with the industry and other stakeholders well in advance and have seen no adverse impact to execution of legitimate porting requests.[22] As the *NPRM* notes, Verizon also proactively notifies consumers of port requests via text message and/or email, which together remain an effective method.[23] For high-risk transactions it may be appropriate to couple notification with the consumer's affirmative verification that he or she requested the port. (Though Verizon's NTP largely supersedes the purpose of a subsequent verification, while enabling timely execution of the port.)[24] Verizon also allows customers to elect a port freeze—though the NTP process is preferable to a freeze, which is dependent on the customer's affirmative action.

Verizon also has processes for tracking, investigating and remediating fraudulent ports.[25] Different unauthorized ports merit different levels of treatment (e.g., certain intra-family disputes on one hand, versus fraud on the other). In this regard, Verizon supports Best Practice 73, which is focused on more serious incidents of fraud and misrepresentation.[26] But Verizon tracks all unauthorized ports to help determine the underlying cause and appropriate remediation, and works closely with other providers to resolve issues and disputes as they arise. These efforts help detect bad actors' new techniques and build new protections going forward.

---

22 *See id.* ¶¶ 49, 53. Occasional customer-specific issues are effectively resolved between providers' porting staffs.

23 *Id.* ¶ 50.

24 *Id.* ¶ 51.

25 *Id.* ¶ 61.

26 *Id.* ¶ 64.

B. Any New Porting Fields Rule Should Preserve Wireless Providers' Flexibility to Take Additional Protective Measures for Customers.

Verizon supports codifying aspects of the "four fields" practice for initiating porting transactions. It is flexible enough to enable the use of the NTP and port freezes, and provides an expeditious port-out process while improving protections available to customers. ZIP code is of limited use for verification given its wide availability, however, and has resulted in unnecessary confusion in porting transactions. And as with SIM changes, any rules in this area should apply on a competitively neutral basis, including for MVNOs and VoIP providers.[27]

Finally, wireless providers require flexibility to quickly adapt their practices to stay ahead of bad actors. The four fields and other wireless porting practices pre-date the heightened level of port-out fraud that prompted the *NPRM*, and standing alone will often not adequately protect customers. For example, while Verizon almost always meets the industry-agreed-upon 2.5 hour period for completing ports by a substantial margin, in limited cases providers may identify security risks that warrant a longer period. And while two-factor authentication procedures are generally appropriate for prepaid as well, the nature of the customer relationship will limit the available authentication options.

III. CONCLUSION

Carefully crafted and limited Commission rules could help give wireless providers some added regulatory certainty in their efforts to combat fraudulent SIM changes and number ports. But providers should retain the flexibility they enjoy today to nimbly adopt new authentication

[27] Verizon does not see a role for the NPAC in this area. The porting fields are part of the process used to obtain the release/confirmation of the port before moving the number from one network to the other in the NPAC. Other than the telephone number, the NPAC does not store these data elements. *See NPRM* ¶ 63.

safeguards to stay ahead of bad actors, while preserving the competitive and consumer benefits for the overwhelming number of lawful SIM changes and ports.

Respectfully submitted,

/s/ Robert G. Morse

William H. Johnson
Of Counsel

Gregory M. Romano
Robert G. Morse
1300 I Street, N.W.
Suite 500 East
Washington, DC 20005
(202) 515-2400

Attorneys for Verizon

November 15, 2021